Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On a Method of Constructing all the Groups of Order p^m.

BY G. A. MILLER.

A group G of order p^m (p being any prime) contains at least one invariant subgroup H of order p^{m-1}. If G is represented as a regular substitution group, then H has p systems of intransitivity and its p transitive constituents ($H_1, H_2, \ldots, H_p$) are transformed cyclically by every substitution of G which is not contained in H. Moreover, there is a substitution t of order p which is commutative with every substitution of H and permutes its transitive constituents cyclically.* It seems desirable, in considering the construction of all the possible groups of order p^m, to divide them into two classes: 1). Those in which the operators of H are transformed only according to the group (I_0) of cogredient isomorphisms of H, and 2). Those in which these operators are transformed according to a larger group.

If G belongs to the first class, it must involve a substitution s which is commutative with each substitution of H and is not contained in H. It may be supposed that t permutes the transitive constituents of H in the same manner as s does. The substitution $st^{-1} = s'$ transforms each of these constituents into itself, and is commutative with every substitution of H. That is, s' is one of the substitutions of the group of order $p^{(m-1)p}$ which is composed of all the substitutions which are commutative with each substitution of H without permuting any of its transitive constituents or involving any letters not found in H.

The group generated by H and $s't$ can be transformed into one generated by H and $s_1 t$, s_1 being a substitution of H_1 which is commutative with every substitution of H_1. Furthermore, the $p-1$ groups of order p^m generated by H and the following substitutions, taken separately,

$$s_1 t, \quad s_1^2 t, \quad \ldots \ldots, \quad s_1^{p-1} t,$$

---

* Cf. Quarterly Journal of Mathematics, vol. XXVIII, 1896, p. 237.

are conjugate, since all of them may be obtained from any one of them by permuting systems of intransitivity of H, the first system being left unchanged. On transforming the group generated by H and t by $r_1^{p-1}r_3r_4^2 \dots r_p^{p-2}$, r_1 being any invariant substitution of H_1 while $r_\alpha\,(\alpha = 2, 3, \dots, p)$ is the transform of r_1 with respect to t^α, there results a group generated by H and $r_1^{-p}t$.

From what precedes, it may be observed that all the possible groups of order p^m, which include H and transform its operators only according to substitutions of I_0, may be obtained by multiplying H by s_1t, where s_1 must satisfy all of the following conditions:[*] 1). It must be an invariant substitution of H_1; 2). If we form the quotient group of these invariant substitutions with respect to the subgroup generated by their p^{th} powers, then it is not necessary to use for s_1 more than one from each of the divisions corresponding to the operators of this quotient group; 3). Not more than one from each system of conjugate operators of H_1 under its holomorph should be used for s_1; 4). The $p-1$ groups generated by H and one of the following operators s_1t, s_1^2t, s_1^2t, $\dots$, $s_1^{p-1}t$ are conjugate; that is, if one substitution is a power of another, it is not necessary to use both for s_1 unless one of them is identity.

When G contains an operator which transforms H according to a substitution (i) which is not contained in I_0, then G transforms the operators of H according to a group I_1 whose order is p times the order of I_0 and which includes I_0. Let $t_1t_2 \dots t_p$ transform the constituents of H according to i. Since i^p must be in I_0, $(t_1t_2 \dots t_p)^p$ must transform H in the same manner as one of its own substitutions s' transforms H. Suppose that s' is commutative with $t_1t_2 \dots t_p$ and that $s_1, s_2, \dots, s_p$ represent its constituents contained in $H_1, H_2, \dots H_p$ respectively. The substitution $t_1^{-p}s_1 = s_1'$ is commutative with every substitution of H. Hence $s_1't_1t_2 \dots t_pt$ transforms the substitutions of H in exactly the same manner as $t_1t_2 \dots t_p$ does. Moreover, $(s_1't_1t_2 \dots t_pt)^p = s'$, From this it follows that H and $s_1't_1t_2 \dots t_pt$ generate a group in which H is transfomed in the required manner.

The assumption that there is a substitution s' in H which is commutative with $t_1t_2 \dots t_p$ and transforms H in exactly the same way as $(t_1t_2 \dots t_p)^p$ does, is clearly a consequence of the existence of G and hence does not limit the generality of the method. If H is fully known, its group of isomorphisms I can readily be determined, and the subgroups which satisfy the conditions imposed upon I_1 can be found. In fact, it is only necessary to determine one of the subgroups whose order is the highest power of p that divides the order of I, since only one from each system of such subgroups as I_1, which are conjugate under I, needs to be considered. Furthermore, it is necessary to consider only the substitutions which may correspond to any particular one of the operators (not in I_0) of such a subgroup. It remains, therefore, only to examine all the possible groups which may be obtained by replacing $s_1' t_1 t_2 \ldots\ldots t_p t$ by other substitutions which transform it in the same manner.

---

[*] Cf. **Transactions of the American Mathematical Society. vol. II, 1901, p. 264. It should be observed that H is not necessarily Abelian in the present article.**

Any one of these substitutions may be transformed into $s_1' t_1 t_2 \ldots\ldots t_p t$ multiplied by a substitution which involves only the letters of H_1 and is commutative with each of the substitutions of H_1. In order that the p^{th} power of such a product may be in H_1, it is necessary that this multiplier is an invariant substitution of H_1 and is also commutative with t_1. Let any one of these products be denoted by $s_1'' t_1 t_2 \ldots\ldots t_p t$. No new group is obtained by using in place of s_1'' any of its conjugates under the subgroup of the group of isomorphisms of H_1 which includes all its operators that are commutative with t_1. When H_1 is Abelian, these conjugates include all the powers of s_1'' which are prime to its order.*

Let r_1 be an invariant substitution of H_1, and let

$$t_1 r_1 t_1^{-1} = u_1 r_1, \quad t_1 u_1 t_1^{-1} = u_1, \quad u_1^p = 1, \quad p > 2,$$

where u_1 does not necessarily differ from identity. Hence

$$(r_1^{p-1} r_3 r_4^2 \ldots\ldots r_p^{p-2})^{-1} s_1' t_1 t_2 \ldots\ldots t_p t r_1^{p-1} r_3 r_4^2 \ldots\ldots r_p^{p-2}$$
$$= s_1' r_1^{1-p} r_2 r_3 \ldots\ldots r_p u_2 u_3^2 u_4^3 \ldots\ldots u_p^{p-1} t_1 t_2 \ldots\ldots t_p t.$$

Transforming succsseively by u_p^{p-1}, u_{p-1}^{2p-3}, ... and multiplying into $(r_1 r_2 \ldots r_p)^{-1}$ there results $s_1' r_1^{-p} t_1 t_2 \ldots\ldots t_p t$. Hence no additional group is obtained by multiplying $s_1' t_1 t_2 \ldots\ldots t_p t$ by the p^{th} power of such an r_1. That is, if the quotient group of the invariant substitutions of H_1, which are commutative with t_1, are arranged with respect to the p^{th} powers of such substitutions as r_1, then no more than one substitution from each of these divisions needs to be used as a multiplier of $s_1' t_1 t_2 \ldots\ldots t_p t$.

When $p = 2$, the results of the preceding paragraph remain true, provided u_1 is either 1 or a power of r_1. In the latter case the order of r_1 must exceed 4.

---

* Transactions of the American Mathematical Society, vol. II, 1901, p. 260.

When $p > 3$, these results still remain true if u_1 is replaced by any substitution (y_1) such that $t_1 y_1 t_1^{-1} = x_1 y_1$, $t_1 x_1 t_1^{-1} = x_1$, $x_1^p = y_1^p = 1$. It should be observed that it is not proved that all the groups of order p^m obtained, in the above manner, from a particular group of order p^{m-1} are distinct. In general, additional limitations must be imposed upon s''. However, the special considerations for small values of m are sufficiently limited to make the method practicable. For instance, when $m < 5$ and $p > 3$, only one non-Abelian group will occur twice if we use for the subgroup of order p^{m-1} the different Abelian groups of order p^{m-1}.

STANFORD UNIVERSITY, *Dec.*, 1901.